

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

NAGRAVISION SA and
NAGRASTAR LLC

Plaintiffs,

v.

DOES 1-100

Defendants.

§
§
§
§
§
§
§
§
§
§

CIVIL ACTION NO. _____

JURY

PLAINTIFFS' ORIGINAL COMPLAINT

Plaintiffs Nagravision SA and NagraStar LLC bring this suit against Defendants for violation of the Digital Millennium Copyright Act and the Communications Act.

INTRODUCTION & NATURE OF THE ACTION

1. Nagravision is a world leader in digital content security. Nagravision provides proprietary software codes, processes, and technologies including its patented International Data Encryption Algorithm ("IDEA") contained within "smart cards" ("Access Cards"), satellite receivers, and terrestrial or cable set-top boxes to encrypt and secure its customers' subscription based television programming. In North America, Nagravision provides conditional access technology to subscription based television operators including DISH Network, Bell TV, Globecast, Dish Mexico, and Cable ONE. Nagravision also provides conditional access technology to numerous subscription based television operators in South America, Europe, and Asia.

2. NagraStar provides DISH Network and Bell TV with Access Cards that contain Nagravision's proprietary software codes, processes, and technologies within a microprocessor component that functions as a security computer to DISH Network and Bell TV's conditional access system. These Access Cards and related encryption technology are utilized in the satellite receivers that DISH Network and Bell TV's consumers either purchase or lease.

3. Defendants are satellite pirates who use and distribute technology, software tools and files that enable individuals to circumvent Plaintiffs' conditional access technology and intercept and decrypt Plaintiffs' customers' digital pay TV programming without authorization and without payment of subscription fees to the digital pay TV operator.

4. Defendants' conduct violates a variety of federal statutes, including the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1) and the Communications Act, 47 U.S.C. § 605(e)(4).

5. Plaintiffs bring this suit seeking civil impoundment of Defendants' software tools and files and related computers and materials under the impoundment provisions of the Digital Millennium Copyright Act, for a preliminary and permanent injunction barring Defendants from trafficking in such devices, and for such other relief as Plaintiffs prove themselves entitled.

JURISDICTION AND VENUE

6. This court has original federal question subject matter jurisdiction under 28 U.S.C. §§ 1331 because the claims are based upon the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.* and the Communications Act of 1934, as amended, 47 U.S.C. § 605 *et seq.*

7. Venue in this District is proper under 28 U.S.C. § 1391(b) and 28 U.S.C. § 1400(a). Although the true identity of each Defendant is unknown to Plaintiffs at this time, on information and belief, each Defendant may be found in this District and/or a substantial part of the acts complained of herein occurred in this District. On information and belief, personal jurisdiction in this District is proper because each Defendant, without consent or permission of Plaintiffs distributed and offered to distribute technology, software tools and files that enable consumers to illegally intercept Plaintiffs' conditional access technology that protects access to copyrighted works in this jurisdiction.

PARTIES¹

8. Plaintiff NagraVision SA is a corporation organized and existing under the laws of Switzerland. NagraVision SA's principal place of business is at 22-24, Route de Genève, 1033 Cheseaux, Switzerland and it is listed on the SIX Swiss Exchange under the symbol "KUD.VX." NagraVision SA is a Kudelski Group company headquartered in Switzerland.

9. Plaintiff NagraStar LLC is a Colorado limited liability company with its principal place of business located at 90 Inverness Circle East, Englewood, Colorado 80112, Arapahoe County. NagraStar is a joint venture between EchoStar Corporation and the Kudelski Group. NagraStar LLC's sole members are EchoStar Corporation and Kudelski SA. EchoStar Corporation is a Nevada Corporation that is publicly owned and traded on the NASDAQ national market under the symbol "SATS." Kudelski SA has its principal place of business at 22-24, Route de Genève, 1033 Cheseaux, Switzerland and is listed on the SIX Swiss Exchange under the symbol "KUD."

10. The true names of Defendants are unknown to Plaintiffs at this time. Each Defendant is known to Plaintiffs only by the Defendant's website and Internet Protocol ("IP") address assigned to that Defendant by his or her Internet Service Provider on the date and at the time at which each Defendant was observed distributing and offering to distribute over the Internet technology, software tools and files that enable consumers to illegally intercept and decrypt Plaintiffs' conditional access technology. Plaintiffs believe that information obtained in discovery will lead to the identification of each Defendant's true name and permit Plaintiffs to amend this Complaint to state the same. Plaintiffs further believe that the information obtained in discovery will lead to the identification of additional parties to be added to this Complaint as

¹ Plaintiffs' allegations related to the wrongful conduct of Defendants are based upon the investigation Plaintiffs have completed to date, upon information and belief, and with the reasonable belief that further investigation and discovery in this action will lead to additional factual support. Plaintiffs therefore expressly reserve their right to supplement, amend and/or otherwise modify their claims and the basis thereof, as additional investigation and discovery is conducted.

defendants since Plaintiffs continue to monitor the Internet distribution of software tools and files that enable consumers to illegally intercept and decrypt Plaintiffs' conditional access technology.

FACTS

11. NagraVision is a world leader in digital content security. Plaintiffs' customers include DISH Network in the United States and Bell TV in Canada. NagraVision's other North American customers include Cable ONE, Dish Mexico, and Globecast. NagraVision's South American customers include NET, Telefonica, TVA, and Via Embratel. NagraVision's European customers include Cyfra+, Canal+/Canalsat, Digital+, Gol-TV, HD+/APS, KDG, Mediaset, Polsat, RCS, Sky Germany, Top-Up TV, UPC, Virgin Media, and ZON-TV. NagraVision's Asian customers include BGCTV, Hong-Kong Cable, Hot, Reliance, SkyLife, and Starhub. Plaintiffs' customers will be collectively referred to as Pay TV Operators.

12. To provide consumers with a variety of programming channels, Pay TV Operators contract for and purchase the distribution rights to copyrighted programming—such as movies, sports, news, and general entertainment programming—from network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other content providers.

13. Because Pay TV Operators generate revenues through the sale of subscription packages and pay-per-view programming, and because the ability to attract and retain distribution rights for programming is dependent upon preventing unauthorized reception of such programming, their video channels (except for certain promotional channels) are digitally secured and encrypted.

14. Plaintiffs' protect Pay TV Operators' programming from unauthorized viewing by using management and security systems, which serve two interrelated functions: (1) subscriber-management—allowing Pay TV Operators to “turn on” or “turn off” programming that a subscriber ordered, cancelled, or changed; and (2) encryption—preventing individuals or entities who have not purchased programming from viewing it.

15. Plaintiffs' security system is composed of two parts. First Pay TV Operators utilize Plaintiffs' technology to encrypt (electronically scramble) their satellite signals using proprietary technology provided by Plaintiffs. To decrypt or descramble this encrypted programming, Plaintiffs provide their customers with "smart cards" ("Access Cards") that contain NagraVision's proprietary software codes, processes, and technologies within a microprocessor component that functions as a security computer to a "conditional access system" known as Digital Nagra Advanced Security Process ("DNASP"). These Access Cards and related encryption technology are utilized in the cable, terrestrial or satellite receivers that consumers either purchase or lease. Second, the DNASP uses a complex encryption system that is combined with a Digital Video Broadcasting scrambler/encoding system to effectively protect and encrypt the Pay TV Operators' programming.

16. A consumer wishing to subscribe to and receive Pay TV Operators' programming must first have the necessary equipment which consists primarily of an integrated receiver/decoder ("receiver") and a credit card-sized Access Card that is loaded into the receiver through a slot on the face of the receiver. On some newer models, the Access Card is integrated directly into the satellite receiver itself and is not removable.

17. The receiver is connected to a cable, fiber optic line, terrestrial antenna or satellite dish to receive signals from the Pay TV Operator. The receiver processes and descrambles the incoming signal using the data and encryption technology stored in the Access Card.

18. Pay TV Operators provide their Access Cards to consumers for use with the receivers for the purpose of enabling authorized access to their programming. Without a subscription, Pay TV Operators will not provide a consumer an Access Card or authorize access to their encrypted programming. Consumers are not authorized to modify or tamper with the Access Card.

19. The Access Card is essential to the operation of the receiver because it contains a secure embedded microprocessor that essentially functions as a security computer, with

proprietary keys and software that contain Nagravision's technology codes used to communicate with the receiver and descramble Pay TV Operators' programming.

20. Nagravision's technology codes within each Access Card are supported by two code segments of memory: Read-Only-Memory ("ROM"); and Electronically Erasable Programmable Read-Only-Memory ("EEPROM"). Generally, the ROM code segment contains the intimate knowledge and information regarding the security system and how it works; whereas the EEPROM code segment contains the secret keys enabling the decryption of the programming.

21. The ROM code segment provides detailed instructions and commands to the Access Cards and receivers in the normal operation of the security system. Access to the proprietary information stored in the ROM code is necessary to unlock the safe containing the secrets to each security system.

22. The EEPROM code segment stores data and command codes that have been written to the Access Cards which the ROM code reads from to perform its calculation and operation functions. Moreover, the EEPROM code segment contains secret keys including, but not limited to "transmission" keys and "pairing" keys (collectively known as "Security Keys"). The Security Keys are used, *inter alia*, to encrypt and decrypt the communications between the Access Card and the receiver.

23. Pay TV Operators communicate with the microprocessor in each Access Card by sending and receiving electronic signals by satellite, cable, or fiber which are routinely updated. The information transmitted to and temporarily stored on the Access Card includes the most recent Security Keys and software necessary to view Pay TV Operators' programming.

24. Plaintiffs' conditional access technology effectively controls access to Pay TV Operators' copyrighted programming. In addition, Plaintiffs' conditional access technology ensures that the protection afforded to such copyrighted works, such as limitations on the dissemination and use in accordance with Pay TV Operators' contractual agreements with

content providers, is preserved. Plaintiffs' conditional access technology is necessary to prevent unauthorized access to Pay TV Operators' programming.

25. The theft of encrypted signals and accompanying programming is commonly referred to in the industry as "satellite piracy" (or "piracy"). Piracy is a problem that costs Plaintiffs and their Pay TV Operators tens of millions of dollars annually in the form of lost revenue, lost subscribers, development and implementation of additional security features and electronic counter-measures (or "ECMs") aimed at disabling pirate devices, and the investigation and prosecution of the individuals responsible for the manufacturing, distribution and use of such pirate devices.

26. Defendants are involved in and/or are responsible for designing, developing, manufacturing, distributing, trafficking-in, and promoting pirate tools and software through their websites. Defendants' technology, software tools and files are primarily designed to, and do, allow end-users to circumvent Plaintiffs' conditional access technology and gain unauthorized access to copyrighted works distributed by Pay TV Operators. This circumvention occurs without authorization or permission from Plaintiffs or their Pay TV Operators.

27. Defendants' pirate technology, tools and software (a) are primarily designed or produced for the purpose of circumventing Plaintiffs' conditional access technology to gain access to Pay TV Operators' programming; (b) have only limited commercially significant purpose or use other than to circumvent Plaintiffs' conditional access technology to gain access to Pay TV Operators' programming; or (c) are marketed by Defendants and/or others acting in concert with Defendants for use in circumventing Plaintiffs' conditional access technology to gain access to Pay TV Operators' programming.

28. Defendants have participated in and/or are responsible for distribution of numerous versions of pirate tools and software. There is no legitimate use for the pirate technology, tools and software distributed by Defendants. Defendants' pirate technology, tools and software have no commercially significant use or purpose. The only use for Defendants' pirate tools and software is to circumvent Plaintiffs' conditional access technology.

CLAIMS FOR RELIEF

COUNT 1

(Manufacture, Import, Offer to the Public, Provide, or Otherwise Traffic in Technologies, Products, Services, Devices, Components, or Parts Thereof in Violation of the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1))

29. Plaintiffs incorporate the preceding paragraphs as if set forth herein.

30. Defendants were and are actively engaged in distributing unlawful technologies, products, services, components, or parts thereof in violation of the DMCA, 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1).

31. Defendants' pirate technology, tools and software are: (1) designed or produced for the purpose of circumventing Plaintiffs' conditional access technology—a technological measure that effectively controls access to, copying and distribution of, copyrighted works; (2) made available by Defendants despite having no commercially significant purpose or use other than to circumvent Plaintiffs' conditional access technology; and/or (3) marketed by Defendants and/or through others acting in concert with knowledge that they are used to circumvent Plaintiffs' conditional access technology.

32. Defendants were and are distributing pirate technology, tools and software with knowledge that these technologies, products, services, components, or parts thereof are used to circumvent Plaintiffs' conditional access technology.

33. Defendants' actions that constitute violations of the DMCA were performed without permission, authorization, or consent of Plaintiffs, Pay TV Operators, or any owner of copyrighted programming broadcasted on the Pay TV Operators' platform.

34. Defendants violated Sections 1201(a)(2) and 1201(b)(1) of the DMCA willfully and for purposes of commercial advantage or private financial gain.

35. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the court, Defendants will continue to violate Sections 1201(a)(2) and 1201(b)(1) of the DMCA.

COUNT 2

**(Manufacture and Sale of Signal Theft Devices and Technology in Violation of the
Communications Act, 47 U.S.C. § 605(e)(4))**

36. Plaintiffs incorporate the preceding paragraphs as if set forth herein.

37. Defendants were and are engaged in the designing, manufacturing, developing, assembling, modifying, importing, exporting, selling, or otherwise distributing pirate tools and software to facilitate the illegal use and reception of Pay TV Operators' programming in violation of the Communications Act, 47 U.S.C. § 605(e)(4).

38. Defendants were and are assisting, directly or indirectly, with the design, manufacture, development, assembly, modification, solicitation, and/or distribution of pirate tools and software with knowledge, or having reason to know, that such devices and technology were and are used primarily to assist in the unauthorized interception and decryption of direct-to-home satellite services in violation of the Communications Act, 47 U.S.C. § 605(e)(4).

39. Defendants violated Section 605(e)(4) of the Communications Act willfully and for the purpose of direct or indirect commercial advantage or private financial gain.

40. Defendants' misconduct has and will continue to cause damage to Plaintiffs in an amount to be proven at trial. Unless permanently restrained and enjoined by the court, Defendants will continue to violate the alleged provisions of the Communications Act.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs seeks judgment against Defendants as follows:

A. For a grant of permanent injunctive relief restraining and enjoining Defendants, and their employees, agents, representatives, attorneys, and all persons acting or claiming to act on their behalf or under their direction or authority, and all persons acting in concert or in participation with them, from:

1) offering to the public, providing, or otherwise trafficking in any pirate technology, tools or software, or any other device, component, or technology, or part thereof, through any means including Internet websites, that:

a) is primarily designed or produced for the purpose of circumventing Plaintiffs' conditional access technology, including the encryption and access control protection contained in the software on any Pay TV Operators' Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on any Pay TV Operators' platform;

b) have only a limited commercially significant purpose or use other than to circumvent Plaintiffs' conditional access technology, including the encryption and access control protection contained in the software on any Pay TV Operators' Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on any Pay TV Operators' platform;

c) is knowingly marketed by Defendants and/or others acting in concert with Defendants for use in circumventing Plaintiffs' conditional access technology, including the encryption and access control protection contained in the software on Plaintiffs' any Pay TV Operators' Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on any Pay TV Operators' platform; and

2) assembling, modifying, selling, and/or distributing any pirate technology, tools or software knowing or having reason to know that such device or software is primarily of assistance in the unauthorized decryption of direct-to-home satellite services through any means including Internet websites;

3) receiving any Pay TV Operators' electronic communications without authorization through any means; and

4) assisting others in receiving (including assistance offered by providing hypertext links or banner advertising) any Pay TV Operators' electronic communications without authorization through any means including the Internet.

B. For an Order impounding all copies, electronic or otherwise, of pirate tools or software or other circumvention or signal theft technology, components, or devices in the

custody or control of Defendants or related entities that the court has reasonable cause to believe were involved in a violation of the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.*

C. For an Order directing Defendants to preserve and maintain all records, in any form (including electronic form), that evidence, refer, or relate to: pirate technology, tools or software, communications or correspondence with suppliers of software, hardware, or other equipment or know-how concerning satellite television piracy.

D. Award Plaintiffs the greater of their actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the amount of up to \$100,000 for each violation of 47 U.S.C. § 605(e)(4), pursuant to 47 U.S.C. § 605(e)(3)(C)(i).

E. Award Plaintiffs the greater of their actual damages together with any profits made by Defendants that are attributable to the violations alleged herein, or statutory damages in the amount of up to \$2,500 for each violation of 17 U.S.C. §§ 1201(a)(2) and 1201(b)(1), pursuant to 17 U.S.C. §§ 1203(c)(2) and 1203(c)(3)(A).

F. For an award of Plaintiffs' costs, reasonable attorneys' fees, and investigative fees.

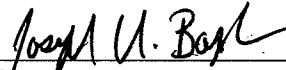
G. For pre- and post-judgment interest on all profits and damages granted by this court in accordance with the law.

H. For such other and further relief as the court deems just and proper.

DATED: November 3, 2010

Respectfully submitted,

HAGAN NOLL & BOYLE LLC

By: 
Joseph H. Boyle (Attorney-In-Charge)
Texas Bar No. 24031757
Southern District of Texas Bar No. 30740
Two Memorial City Plaza
820 Gessner, Suite 940
Houston, Texas 77024
Telephone: (713) 343-0478
Facsimile: (713) 758-0146

Stephen M. Ferguson (Of Counsel)
Texas Bar No. 24035248
Southern District of Texas Bar No. 614706

COUNSEL FOR PLAINTIFFS
NAGRAVISION SA and
NAGRASTAR LLC